DRAFT

COMMON CRITERIA TESTING PROGRAM
DERIVED TEST REQUIREMENTS
OF THE US GOVERNMENT
APPLICATION LEVEL FIREWALL PROTECTION PROFILE
FOR LOW RISK ENVIRONMENTS

Prepared for the National Institute of Standards and Technology
Under Contract Number DCA100-95-D-0104

James Arnold
Ronald Koch
Christopher Kostick
Frank Mayer
Daniel Tapper
Robert Williamson

15 April, 1998
Version 1.0

SAIC®
Science Applications International Corporation
An Employee-Owned Company
6740 Alexander Bell Drive Suite 350 Columbia, MD 21046 (410) 872-4700 Fax (410) 872-0107

Document Conventions

The notation, typographic conventions, and definitions used in this Derived Verification Requirements (DTR) document are consistent with the Application Level Firewall Protection Profile.

Application Level Firewall Protection Profile requirements are written in *Italics*. For example,

> *FIA_ATD.2.1 The TSF shall provide,* ***for each authorized administrator, trusted host, host, and user that is defined to it****, a unique set of security attributes necessary to enforce the TSP.*

The DTR notes, written in normal text, are written into three separate action-item sections for each requirement—inputs, evaluator design analysis**,** and testing. The section, **inputs** describes information a vendor needs to provide for the specific requirement. The **design analysis** section identifies the analysis an evaluator must undertake for determining if the TSF meets the requirement. The **testing** section describes tests the evaluator needs to perform. For some requirements, a fourth section, **interpretations** appears. The interpretation section is present in this draft DTR; however it is anticipated that once a firewall is evaluated, that this DTR will be finalized and the interpretations sections will disappear.

1. Introduction

This Derived Test Requirements (DTR) document recommends and discusses the actions evaluators should take when evaluating products against the Application Level Firewall Protection Profile Low Risk Environments (hereafter referred to as the PP).

1.1 Purpose

The intent of the PP is to specify features, mechanisms, and assurances applicable to application level firewalls. The intent of this DTR is to provide evaluator guidance and recommend actions to take in order to determine a product's compliance with the features and mechanisms of the PP. Specifically, it identifies what evaluators should do to confirm that each requirement from the PP has been met.

The objective behind providing this guidance to evaluators is to standardize the approach followed in evaluating firewall products against the PP to ensure consistency across all evaluations. Evaluation consistency refers to the consistent interpretation of requirements as well as a consistent level of analysis throughout the evaluation process.

To provide a context for evaluator actions, a description is given of information the vendor is expected to provide about the Target of Evaluation (TOE) with respect to each functional and documentation requirement. The descriptions of expected vendor information (except for those statements quoted verbatim from the PP) do not constitute requirements.

The consistent application of the PP requirements and the evaluation process is also intended to support consistent management decisions as to whether a product is fit to include on the evaluated products list by ensuring that no evaluation team is held to a higher standard or level of analysis than any other team.

1.2 Approach

This DTR makes no statement about the level of trust or the security features of the hardware and operating system used to support the firewall evaluated against this DTR. However, it should be realized that no security features of the firewall will work correctly if the operating system does not work correctly. It is the operating system that provides all of the resources used by the firewall software. The operating system will not work correctly if the hardware does not work correctly. It is the hardware that translates operating system abstractions (e.g., virtual address space) into hardware realities (physical page of memory).

If the firewall evaluated against this DTR is to be assessed at a specific level of assurance[1], the hardware (e.g., CPU, motherboard, communication cards, peripheral cards, printer, encryption device) and the software (e.g. operating system, database management system, audit reporting tool), on which the firewall requests services, must all be evaluated at the same or higher level of assurance. This point is fundamental to the level of trust that can be placed in the firewall and it

[1] Common Criteria Testing Program Derived Test Requirements For EAL1 Through EAL3, draft 11, March 1998.

is often misunderstood. Even if the firewall can be ported to a new platform and all functional tests run correctly, the assurance that the firewall will meet the requirements in this DTR is no higher than the lowest assurance level of the underlying hardware and software that provide the resources to the firewall for it to execute.

As stated above, the DTR notes are written into three separate action-item sections for each requirement—inputs, design analysis and testing. The testing section sometimes describes descriptive tests and at other times describes prescriptive tests. Descriptive tests are required to be performed by the evaluator. Prescriptive tests are provided as a recommended method for testing the requirement and are the types of tests that have been used to successfully test mechanisms designed to meet similar requirements. If a prescriptive test cannot be executed, the evaluator should determine the reason for the test (often stated) and design an equivalent test for the specific TOE being evaluated.

This DTR only addresses the functional requirements for the PP. It is not the purpose of this DTR to discuss the assurance requirements associated with the PP. Rather, assurances are described in the document, *Common Criteria Testing Program: Derived Test Requirements For EAL1 Through EAL3*, Version 1.0, dated 11 March 1998. This firewall DTR references documents that are identified, in that document, to be provided by the vendor. The documents listed as required for EAL2 that are referenced in this DTR are as follows:

- Functional Specification (FSPEC),
- TOE Security Policy (TSP),
- High-level Design (HLD),
- Administrator Guidance (AG),
- Test coverage analysis,
- Test plans, test procedures, and test results,
- Strength of Security Function Analysis, and
- Vulnerability analysis.

Assurances are briefly described in Section 3 of this firewall DTR to provide a brief introduction of the material that is discussed in the *Derived Test* R*equirements For EAL1 Through EAL3.*

1.3 Firewall Security Policies[2]

When performing a security analysis for an operating system or a Database Management System (DBMS), subjects typically are active entities running on behalf of a user (e.g., process). In a firewall, unless untrusted applications are allowed, the only internal active entity running on behalf of a remote untrusted user may be a proxy, or a protocol providing a service. None, of these subjects, are running on behalf of the untrusted user, and no subjects may run on behalf of an untrusted user unless untrusted applications are allowed on the firewall. When an untrusted user is considered a subject in a firewall, it is the service requested over a connection by an

[2] The genesis of this discussion can be found in Appendix A of the *Final Evaluation Report for the Milkyway Networks Black Hole Firewall Version 3.01E2-for SPARCstations,* issued by the Communications Security Establishment (CSE) of Canada on November 1997.

untrusted user that is the subject. In that request, the user must somehow be identified, so the firewall can make a determination whether to connect this request to the service provider.

There is a similar problem when trying to define objects on a firewall if the criteria used is the same as used for an operating system or DBMS. Typically, in a firewall, untrusted users have no interface to directly access data, unless untrusted applications are allowed and can create objects. Rather, an untrusted user is granted a communication path through a firewall. Therefore, any data referenced on behalf of the user is data necessary to support the protocol, proxy, or service routine. Objects, are typically a communication path to a service; a connection. When a host is considered an object in a firewall, the firewall has no control over the host or the objects (e.g., files data sets), but rather the firewall controls the connection to the host that was requested by the user or other host over a connection to the firewall.

When an active entity (e.g., process) running on the firewall is providing a service for an authorized administrator or Trusted Host that entity is the considered a subject, and these subjects are very similar to subjects in an operating system or DBMS. The authorized administrator and trusted host are provided direct access, through a TSF interface, to named objects like files and data sets. These named objects are typically the routing or connection tables, user identity tables, user service table, and, if untrusted applications are allowed, user authentication data.

Throughout this DTR, the terms subjects and objects appear. At times the term services will be used to indicate an object in the context of a firewall. When this occurs, the word object in parenthesis will always follow services. When, either the term subject, object, or services is used in this DTR, consideration must be given that these terms are being used in the context of a firewall.

A few terms used to identify subjects need to be clarified before the reader progresses through this DTR. An **authorized administrator** is a person who is identified as a person authorized to perform administrative activities on the firewall. This person is identified to the firewall during initialization and the firewall must know the identity of this person the entire time the firewall is connected and providing services. An authorized administrator is authorized to perform activities on the firewall that will violate the requirements of the Security Target (violate the TSP). An authorized administrator must be authenticated in some way, so the firewall has the assurance that the person claiming to be the administrator actually is the administrator.

A **trusted host** is a remotely connected host where an active entity communicating with the firewall may perform administrative duties on the firewall. A trusted host must be authenticated and the TSF must provide, to the trusted host, interfaces to the same administrative routines that are provided by the TSF to the authorized administrator.

An **untrusted user** is any user who is not an authorized administrator. This term does not reflect on the person’s personnel qualities; but rather that the person is not trusted by the firewall to perform activities that can violate the TSP.

A **host** is a remotely connected host that is not authorized on the firewall. Typically such a host is requesting network services and is using the firewall as a router.

2. Firewall Functional Security Requirements

This section provides functional requirements that must be satisfied by a PP-compliant firewall.

The functional security requirements for this PP consist of the components summarized in Table 2.1.

Functional Class	Functional Components
User Data Protection	FDP_ACC.2, Complete Object Access Control FDP_ACF.4, Access Authorization and Denial FDP_ACF.2, Multiple Security Attribute Access Control FDP_RIP.3, Full Residual Information Protection on Allocation FDP_SAM.1, Administrator Attribute Modification FDP_SAQ.1, Administrator Attribute Query
Identification and Authentication	FIA_ADA.1, User Authentication Data Initialization FIA_ADP.1, Basic User Authentication Data Protection FIA_AFL.,1 Basic Authentication Failure Handling FIA_ATA.1, User Attribute Initialization FIA_ATD.2, Unique User Attribute Protection FIA_UAU.1, Basic User Authentication FIA_UAU.2, Single-use Authentication Mechanism FIA_UID.2, Unique Identification of Users
Cryptographic Support	FCS_COP.2, Standards-Based Cryptographic Operation
Protection of the Trusted Security Functions	FPT_RVM.1, Non-Bypassability of the TSP
	FPT_SEP.1, TSF Domain Separation
	FPT_TSA.2, Separate Security Administrative Role FPT_TSM.1, Management Functions
Security Audit	FAU_GEN.1, Audit Data Generation FAU_MGT.1, Audit Trail Management FAU_POP.1, Human Understandable Format FAU_PRO.1, Restricted Audit Trail Access FAU_SAR.1, Restricted Audit Review FAU_SAR.3, Selectable Audit Review FAU_STG.3, Prevention of Audit Data Loss

Table 2.1 Functional Security Requirements

2.1 FDP User Data Protection

Two Security Function Policies (SFPs) must be addressed for each requirement of the User Data Protection class of functional security requirements. One SFP, called UNAUTHENTICATED_END-TO-END-POLICY (*unauthenticated policy*), describes a connection where the subject is a host unauthenticated to the TOE. The other SFP, called the AUTHENTICATED_END_TO_END_POLICY (*authenticated policy*) describes a connection where the subject is an untrusted user, authorized administrator or trusted host authenticated to the TOE.

2.1.1 *FDP_ACC.2 Complete Object Access Control*

FDP_ACC.2.1 The TSF shall enforce the ***[UNAUTHENTICATED_END-TO-END_POLICY]****, on:*

a) [The subjects: hosts not authenticated at the TOE];
b) [The objects: hosts on the internal and external network(s)];

[and all operations among subjects and objects covered by the Security Function Policy (SFP)].

Inputs:

The vendor should provide documentation that describes the following:

- packet parameters that identify an uauthenticated host as a subject (e.g., network address, host name, network identifier, connection id);

- how an uauthenticated host is identified as an object on an internal network, and an external network[3] and how a host is identified as an authenticated (trusted) host on an internal network;

- the ability of the Target of Evaluation (TOE) to enforce an unauthenticated policy for services between the following:

  a) two unauthenticated external hosts4;

  b) an unauthenticated external host requesting services to an internal unauthenticated host; and

  c) an unauthenticated external host requesting services of an internal trusted host.

- how the TSF determines the unique identity of an unauthenticated external host even if it has the source address of an internal host, and how the TSF reacts to this situation;

- all operations allowed between an unauthenticated external host and another host (unauthenticated external or internal host or a trusted host).

[3] The location attribute is required to meet this requirement and requirement FDP_ACF.2.2. The terms “location,” “internal,” and “external” are somewhat vague, especially for a firewall configured with interfaces to more than two networks. For this DTR, requirements that address the location of a host are interpreted as follows. Any host with a network address that is outside the range of network addresses associated with the port on which the request was received or for which the request is targeted is a host on an external network. Any host with a network address that is within the range of network addresses associated with the port on which the request was received or for which the request is targeted is a host on an internal network.

[4] Hosts on an external network are called external hosts; hosts on an internal network are called internal hosts.

Design Analysis:

Based on the above requirements, the evaluator must:

- understand what constitutes a valid request for services by an unauthenticated host acting as a subject to a host on an internal or external network;

- perform an object study to identify (or confirm the vendor's identification of) all the types of services (objects) to which the access control policy for unauthenticated hosts applies and how objects are identified. For example, an object may be defined as an internal or external host (destination address), an unauthenticated host or a trusted host, a service (e.g., ftp), or a subset of the service (e.g., ftp "get" or "put"). It should also be noted that a service could be interpreted as access to a network as well;

- understand how a request is associated with an unauthenticated host; and

- determine if the services allowed through the firewall between an unauthenticated host and another host (unauthenticated or trusted) are consistent with the SFP. Either host may be on an internal or external network.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

Evaluator testing for requirement FDP_ACC.2.1 is by analysis. The evaluator must perform the following:

- confirm that unauthenticated hosts are uniquely identified;

- confirm that unauthenticated hosts on internal and external networks can be uniquely differentiated;

- examine how access to each service is mediated by the TSF; and

- confirm that all operations allowed between an unauthenticated host and another host (unauthenticated or trusted) on an internal or external network are consistent with the SFP.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FDP_ACC.2.1 The TSF shall enforce the ***[AUTHENTICATED_END-TO-END_POLICY]****, on:*

a) [The subjects: users authenticated at the TOE].
b) The objects: hosts on the internal and external network(s);

[and all operations among subjects and objects covered by the SFP.

Inputs:

The vendor should provide documentation that describes the firewall's security policy. This description should include:

- description of the Target of Evaluation (TOE) as a product that enforces an authenticated SFP and the state on which the policy is enforced (e.g., session, connection, continuous packet flow without session or connection state);
- description how a user is identified by the TSF and the user abstraction that is authenticated;
- description of the authentication mechanism by which the user is authenticated;
- explanation of what constitutes an object both at the TSF interface and internal within the TSF that participate in the enforcement of the SFP (e.g., external host, internal unauthenticated host, trusted host, port, IP address;
- explanation of how access is mediated between authenticated users and hosts and what constitutes authorized access;
- description of all operations allowed between an authenticated user and an external host or an unauthenticated or trusted host;
- identification of the TOE Security Functions (TSF) interface; and
- identification of security-relevant attributes used to make access controls decisions and the manner in which these attributes are associated with an object.

Design Analysis:

Based on the above requirements, the evaluator must:

- confirm the user abstraction is authenticated by the TSF;
- perform an object study to identify (or confirm the vendor's identification of) the types of services (objects) to which the access control policy for authenticated users applies and how objects are identified. For example, an object may be defined as an internal or external host (destination address), an unauthenticated host or a trusted host, a service (e.g., ftp), or a subset of the service (e.g., ftp "get" or "put"). It should also be noted that a service could be interpreted as access to a network as well;
- understand what constitutes a valid request for access by an authenticated user;
- understand how a request is associated with an authenticated user;

- understand what constitutes an authenticated state (in other words, how is the user authentication and any other relevant state information maintained throughout a session); and

- understand how an authenticated state is terminated.

The documents that need to be reviewed to accomplish testing are: the Security Target, the HLD, and the FSPEC.

Testing:

The evaluator must perform the following:

- confirm that users are uniquely identified;

- confirm that a TSF mechanism performs user authentication;

- examine how access to each object is mediated by the TSF;

- confirm that for each object, the access control policy defines the rules for allowing access; and

- confirm that the TOE differentiates between an authenticated and an unauthenticated state such that the state of being authorized is a function of the decision to grant access to an object, and if the SFP is different for authenticated and unauthenticated users, the services provided to authenticated users are consistent with the SFP and are different then services provided unauthenticated users.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FDP_ACC.2.2 The TSF shall ensure that ***all*** *operations between* ***any*** *subject in the TSC and any object in the TSC are covered by the SFP*[5]*.*

Inputs:

The vendor should provide documentation that describes the firewall's security policy. This description should include the following:

- explanation of what constitutes a subject (e.g., unauthenticated hosts, trusted hosts, users, authorized administrators);

[5] A subject of an authenticated flow of traffic over a network (host, connection or user) initiates a request to access a service whose access is mediated by the firewall. In other words, a subject for an authenticated flow of traffic can be either a trusted host (may be necessary for remote administrative hosts (FPT_TSA.2.4)), or a human user (untrusted or authorized administrator). The subject for an unauthenticated connection may only be a hosts and their identities are not authenticated. In all cases, subjects are the entities that originate requests to access services protected by the firewall. Only through the use of encryption can the assumption be validated that the request is a true representation of what the subject initiated, unless the subject is a locally connected administrator.

- explanation of what constitutes a service (object), both at the TSF interface and internal within the TSF that participate in the enforcement of the SFP, (e.g., access to a locally connected port), access to an unauthenticated host, a trusted host, or an external network (network level), access to services above the network level (e.g., ftp), or a subset of the service (e.g., ftp "get" or "put");

- identification of the external interfaces into the Security Target (TSF interface) since these provide the operations between any TSC subject and any TSC object;

- explanation of how access is mediated between subjects and objects and what constitutes authorized access for all authorized subjects; and

- identification of security-relevant attributes used to make access controls decisions and the manner in which these attributes are associated with a service (object).

The vendor should provide documentation and/or tests that demonstrate that no operation between a subject in the TSC and an object in the TSC can bypass the SFP. This requirement is different than FDP_ACC.2.1, in that in FDP_ACC.2.1. the vendor needs to demonstrate that a policy exists and is applied, whereas in FDP_ACC.2.2, the vendor needs to demonstrate completeness. The vendor needs to demonstrate that ***all*** operations between a subject and an object within the TSC are controlled by the TSF and comply with the SFP.

Design Analysis:

Based on the above requirements, the evaluator must do the following:

- confirm the identification of subjects;

- perform an object study to identify (or confirm the vendor's identification of) **all** objects within the TSC and how they are identified[6];

- understand what constitutes a valid request for access by a subject, and how a request is associated with a subject;

- understand the external interfaces into the Security Target (TSF interface) since these provide the operations between subjects and objects with the TSC;

- understand what constitutes an authenticated state (in other words, how is the subject authentication and any other relevant state information maintained throughout a session);

- understand how access is mediated between subjects and services (objects) and what constitutes authorized access for all authorized subjects;

[6] The analysis required to identify objects when satisfying requirement *FDP_ACC.2.1* is to identify the types of services objects. This analysis may be sufficient for the analysis associated with requirement *FDP_ACC.2.2;* however emphasis here is that **all** services (objects) must be identified to meet this requirement. If multiple services are provided by the same TSF interface, each service must be identified.

- understand the security-relevant attributes used to make access controls decisions and the manner in which these attributes are associated with a service (object); and

- understand how an authenticated state is terminated.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the vendor's HLD.

Testing:

The evaluator must ensure that no TSC interface provides access to an object controlled by the TSC whereby the access is not mediated by the TSF.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.1.2 *FDP_ACF.4 Access Authorization and Denial*

FDP_ACF.4.1 The TSF shall enforce the:

- ***[UNAUTHENTICATED_END-TO-END_POLICY, AND]***
- ***[AUTHENTICATED_END-TO-END_POLICY],***

to provide the ability to explicitly grant access based on the value of security attributes of subjects and objects.

FDP_ACF.4.2 The firewall shall enforce the

- ***[UNAUTHENTICATED_END-TO-END_POLICY, AND]***
- ***[AUTHENTICATED_END-TO-END_POLICY],***

to provide the ability to explicitly deny access based on the value of security attributes of subjects and objects.

Inputs:

The vendor's TSF and HLD documentation should identify all security relevant attributes for all subjects and objects within the TSC and describe how those attributes are used to mediate access.

The vendor needs to describe the TSF mechanism that makes the decision to grant or deny access and the functions within the TSF that invoke this mechanism.

Design Analysis:

The evaluator must identify all security relevant attributes for all of the subjects and objects within the TSC. At a minimum, the set of attributes must include a subject identifier (e.g., host ID, IP address, connection ID, user ID), object identifier (host ID, service name, etc.), role and location.

The evaluator must understand how the access control mechanism uses these attributes to explicitly grant and deny access between subjects and objects protected by the firewall. If there are multiple mechanisms that make an access control decision, the evaluator must understand the functionality of each such mechanism and which TSF functions use a specific mechanism.

The evaluator must also understand how multiple access rules are handled so that access to an object by an individual subject is deterministic regardless of the number of groups in which a subject may be placed. Individual access needs to be deterministic when each group in which a subject resides may have the same access to an object, different access, or conflicting access to an individual subject. One evaluator concern to determine access granted is the order of precedence in enforcing the rules (e.g., first match). For instance, if an access rule allows access to all hosts on network xxx.xxx.xxx.100 except xxx.xxx.xxx.110, and another access rule provides access to xxx.xxx.xxx.110, it must be determined whether access is granted to host xxx.xxx.xxx.110.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation. For each TSF interface, the evaluator must confirm that accesses provided by the TSF interface, to any object within the TSC, is consistent with the TSP.

Testing:

The evaluator must determine that every access attempt by a subject to an object is deterministic and consistent with the SFP.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.1.3 *FDP_ACF.2 Multiple Security Attribute Access Control*

FDP_ACF.2.1 The TSF shall enforce the:

- ***[UNAUTHENTICATED_END-TO-END_POLICY],***

to objects based on [source address, destination address, transport layer protocol, and service requested (e. g., source port number and/or destination port number)].

FDP_ACF.2.2 The TSF shall enforce the following ***additional*** *rules to determine if an operation among controlled subjects and controlled objects is allowed*:

a) [The TOE shall reject requests for access or services that originate from an external, unprotected network, but which has the source address of a host on an internal, protected network];

b) [The TOE shall reject requests for access or services that originate from an external, unprotected network, but which has the source address of a host on an internal, broadcast network];

c) *[The TOE shall reject requests for access or services that originate from an external, unprotected network, but which has the source address of a host on an internal, reserved network];*

d) *[The TOE shall reject requests for access or services that originate from an external, unprotected network, but which has the source address of a host on an internal, loopback network]*

Inputs:

Since FDP_ACF.2.1 only addresses hosts on external unprotected networks as subjects, the vendor should provide documentation that describes the following:

- explanation of how an external unprotected network is identified when it has the same source address as a host on an internal protected network, and how the TSF reacts to this situation;
- explanation of how the TSF determines that a packet actually came from an external unprotected network;
- explanation of how each required type of internal network is defined (protected, broadcast, reserved, and loopback);
- explanation of what differentiates types of internal networks: (protected, broadcast, reserved, and loopback)
- explanation of the TSF interfaces that could be used to provide access to the identified types of internal networks;
- explanation of the access mediation mechanism that was invoked; and
- the ability of the Target of Evaluation (TOE) to enforce the *unauthenticated policy*;

Design Analysis:

The evaluator must ensure that the TSF provides the ability to deny access requested **by** a host on an external unprotected network **to** an internal protected network based on the *type* of internal protected network. Therefore the evaluator must understand how the type of internal protected network is defined, how the TSF determines that the remote host made the request from an unprotected external network, which TSF mechanism actually performs the access check, and that the ***unauthenticated policy*** can actually be enforced.

To evaluate compliance to this requirement, it is essential that the evaluator understand the difference in location between internal and external networks. The evaluator must determine how “location” is determined and how “internal,” and “external” are defined for a firewall configured with interfaces to more than two networks. Policy decisions concerning granting access for “external” networks might state: the firewall shall reject requests for access or services if the source address associated with the request is outside the range of network addresses associated with the port on which the request was received.

If source address and port assignment addresses are used to determine “location,” then a third type of request, other than “internal” and “external” can be initiated by the firewall itself using other TSF routines to process the request as a network request to be sent to specific addresses. The location of such a request can be “internal” if the firewall address is associated with a port; however firewall initiated communication can also be “local” rather than “internal”, whereby the source address of the message is not even checked before being sent. Local requests should be covered by a SFP and considered part of the “internal” network.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, so that the combination of evaluator and vendor written tests sufficiently demonstrate that the TOE rejects request to perform the following:

- access or services that originate from an external, unprotected network, but which have the source address of a host on an internal, protected network;

- access or services that originate from an external, unprotected network, but which have the source address of a host on an internal, broadcast network;

- access or services that originate from an external, unprotected network, but which have the source address of a host on an internal, reserved network; and

- access or services that originate from an external, unprotected network, but which have the source address of a host on an internal, loopback network.

  The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FDP_ACF.2.1 The TSF shall enforce the:

- ***[AUTHENTICATED_END-TO-END_POLICY]***

to objects based on [user ID, source address, destination address, transport layer protocol, service requested (e. g., source port number and/or destination port number), and service command (e.g., an ftp “put”)].

FDP_ACF.2.2 The TSF shall enforce the following ***additional*** *rules to determine if an operation among controlled subjects and controlled objects is allowed:*

a) [The TOE shall reject requests for access or services that originate from an authenticated user on an external, unprotected network, but which has the source address of a host on an internal, protected network];

b) *The TOE shall reject requests for access or services that originate from an authenticated user on an external, unprotected network, but which has the source address of a host on an internal, broadcast network];*

c) *[The TOE shall reject requests for access or services that originate from an authenticated user on an external, unprotected network, but which has the source address of a host on an internal, reserved network];*

d) *[The TOE shall reject requests for access or services that originate from an authenticated user on an external, unprotected network, but which has the source address of a host on an internal, loopback network]*

Inputs:

Since FDP_ACF.2.1 only addresses an authenticated user as the subject, the vendor should provide documentation that describes the firewall's security policy for authenticated users originating request from an external unprotected network. This description should include:

- the ability of the Target of Evaluation (TOE) to enforce an *authenticated policy*;
- an explanation of what constitutes an authenticated user and how each is defined internally in the TOE;
- an explanation of how an external unprotected network is identified when it has the same source address as a host on an internal protected network;
- an explanation of what differentiates types of internal networks: (protected, broadcast, reserved, and loopback)
- an explanation of the TSF interfaces that could be used to provide access to the identified types of internal networks;
- an explanation of the access mediation mechanism that was invoked;

Design Analysis:

The evaluator must ensure that the TSF provides the ability to deny access requested by an authorized user on an external unprotected network to an internal protected network based on the ***type*** of internal protected network. Therefore, the evaluator must understand how the type of internal protected network is defined, how the TSF determines that the authorized user makes the request from an unprotected external network, which TSF mechanism actually performs the access check, and that the ***authorized policy*** can actually be enforced.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that the TOE **rejects** requests for the following requests:

- access or services that originate from an authenticated user on an external, unprotected network, and have the source address of a host on an internal, protected network;
- access or services that originate from an authenticated user on an external, unprotected network, and have the source address of a host on an internal, broadcast network;
- access or services that originate from an authenticated user on an external, unprotected network, and have the source address of a host on an internal, reserved network; and
- access or services that originate from an authenticated user on an external, unprotected network, and have the source address of a host on an internal, loopback network]

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.1.4 *FDP_RIP.3 Full Residual Information Protection on Allocation*

FDP_RIP.3.1 The TSF shall ensure that upon the allocation of a resource to all objects any previous information content is unavailable.

Inputs:

The vendor should perform an analysis for residual data on all system resources allocated to one subject and reused by another subject (e.g., stacks, process memory, etc.) and their attributes.

The vendor’s TSF and HLD documentation should provide a detailed description of the object reuse policy. This description typically includes TSF structures such as the free memory list or data management buffers and visible hardware structures, such as processor registers. Also, the description includes how the policy is implemented for each resource under its purview (e.g., completely over-write, cleared to a default value).

The vendor should, for each class of resources, describe the associated data structure and the corresponding mechanisms for ensuring that no residual data can be accessed. These mechanisms involve allocation or de-allocation of storage resources (e.g., disk space, memory, registers). The vendor should describe when the mechanism is invoked that completely obfuscates the data within the identified structures.

The vendor should demonstrate that the object reuse policy is enforced via testing and/or design arguments. Since object reuse mechanisms are often not visible at the TSF interface, testing could involve the use of special test drivers or tools. The vendor may prefer to demonstrate enforcement of object reuse by design arguments. This demonstration is subject to negotiation with the evaluator of detailed information to be supplied and conditions under which design arguments are inadequate.

Design Analysis:

The evaluator must confirm that the vendor's residual information protection policy applies to all resources that are shared and/or reusable among subjects and resources that are used for each subject (e.g., cache, memory, registers, etc.). Such areas can be allocated to a process, de-allocated, and reallocated to another or the same process; data stored during the first allocation must be made inaccessible to the process to which the resource was reallocated, even in cases of serial reuse of the same resource by a process. The evaluator confirms that, for each class of sharable or reusable data area, a policy for preventing access to residual data is stated (e.g., overwrite when allocated, overwrite when de-allocated, prevent read access by a process until the process has written data). The evaluator confirms that the residual information protection policy applies independent of whether the residual data is encrypted, since data encryption is not a substitute for satisfaction of this requirement.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator must confirm that the vendor's implementation of the residual information protection mechanisms is consistent with the design. This typically involves inspecting the test documentation and repeating some of the related tests.

The evaluator must confirm that the vendor has adequately tested (or presented an equivalently strong design analysis argument for) the residual information protection mechanisms described in the design documentation. Typically, the evaluator examines the vendor's test suite with a focus on those tests that test object reuse. Based on this examination, the evaluator is able to adequately determine whether or not the object reuse mechanisms operate in a satisfactory manner.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

If the evaluator and vendor agree that it is most expedient and less prone to error, the source code may be reviewed to determine that residual information is cleared. As an example where reviewing source code may be applicable would be clearing an object when still in one context and then placing new data from another context all in one TSF routine and the source may have to be modified to provide a test.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.1.5 *FDP_SAM.1 Administrator Attribute Modification*

FDP_SAM.1.1 The TSF shall enforce the <u>access control SFPs</u>:

- *UNAUTHENTICATED_END-TO-END_POLICY, and*
- AUTHENTICATED_END-TO-END_POLICY

to provide authorized administrators with the ability to modify:

- *[The association of User IDs with roles (e.g., authorized administrator)];*
- *[access control attributes listed in FDP_ACF.2];*
- *[security relevant administrative data].*

Interpretation;

First, it appears that this requirement should be parsed as, "The TSF shall provide authorized administrators with the ability to modify the access control SFPs". Second, it is not clear that the identity of a role has to be provided through TSF software, but that procedural methods could provide an administrative role. Even though firewall administration may only be allowed to modify the SFP while the firewall is off-line, FPT_TSA.2.2 requires, *"The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF."* However, it appears that this requirement could be met by restricting physical access to a console and if administrative actions can also be restricted to the console, then role separation could be provided procedurally.

Inputs:

The vendor's HLD documentation or administrative guide should describe the access control policy for authorized administrators. That description needs to include the following:

- identification of the administrative interfaces into the TOE;
- identification of the security-relevant administrative data;
- identification of the TSF mechanism that manages security-relevant administrative data;
- identification of the interfaces into the TSF functions that manage the security relevant administrative data;
- the creation and maintenance of roles by the TSF;
- the association of user-ids with roles, if applicable;
- granting specific administrative capabilities to a role;
- creation of new roles by administrators with the appropriate role;
- assignment of a specific ID to a role, if a role is identified by ID; and

- modification of the access control attributes listed in FDP_ACF.2 only by an administrator with the appropriate role.

Design Analysis:

The evaluator must review the FSPEC, TSF, HLD and AG documentation to:

- understand and describe all of the mechanisms that can be used to administer the security relevant administrative data (for example, it may be possible to modify a security-relevant administrative data (e.g., the firewall ruleset) through both a firewall provided GUI and directly through a text editor);

- understand and describe the scope of the security information that can be accessed via these mechanisms;

- understand and describe what constitutes an authorized administrator (e.g., operating system root account, firewall specific administrator account, database system administrator account, access to the console) and whether there are multiple administrator roles, each with a subset of the privileges required to administer the security relevant information; and

- understand and describe the mechanisms that restrict the use of the administration tools to the identified class of authorized administrators.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, Administrator Guidance, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that the TSF, and only the TSF, can create an authorized administrator. Tests must demonstrate that the authorized administrator has capabilities beyond those associated with untrusted subjects that are identified as follows:

- only an authorized administrator can create a role;

- the only way for an authorized administrator to create, modify, or delete a role is through a TSF interface that is restricted for use by the administrator; and

- for each created role, the authorized administrators can modify:

  a) the association of User IDs with roles;
  b) every access control attributes listed in FDP_ACF.2; and
  c) security-relevant administrative data.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.1.6 *FDP_SAQ.1 Administrator Attribute Query*

FDP_SAQ.1.1 The TSF shall enforce the access control SFPs:

- *UNAUTHENTICATED_END-TO-END_POLICY, and*
- *AUTHENTICATED_END-TO-END_POLICY*

to provide authorized administrators with the ability to query:

- [access control security attributes];
- [host names];
- [user names].

Inputs:

The vendor’s FSPEC and HLD documentation should describe the functions provided that allow an authorized administrator the ability to query the current values of all of the access control security attributes managed by the TSF as well as the method used to restrict access to these functions. This description should include a method to ascertain access control security attributes for each named host and each named user identified to the TOE. At a minimum, the security relevant attributes must include the attributes required by FDP_ACF.4.1, FDP_ACF.4.2, and FDP_ACF.2.1.

The vendor’s Administrator Guide should describe how the query functions that are used by the administrator.

Design Analysis:

Ensuring compliance with this requirement is closely linked with the Evaluator Design Analysis described above for FDP_SAM.1. The evaluator must:

- understand and describe the access control security attributes associated with the TOE and controlled by the TSF that need to be queried;

- understand and describe all access control security attributes specific to hosts identified to the TOE;

- understand and describe all access control security attributes associated with users identified in the TOE;

- understand and describe all of the interfaces that provide the ability to query access control security attributes associated with the TOE, hosts identified to the TOE and users identified to the TOE;

- understand and describe what roles are provided with the privilege to query the access control security attributes, host names, and the user names; and

- understand and describe how access to the query functions and/or the access control security attributes, host names, and user names is controlled.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the AG, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that the following information can only be gained through a TSF interface and that only an authorized administrator can query the TOE for the following information:

- for each individual subject that is controlled by the TSF and is described in the SFP, the security attributes for that subject;
- for each individual object controlled by the TSF and identified in the SFP, the access control security attributes for that object;
- all host names known to the TOE; and
- security attributes associated with all users that have an associated User-ID identified to the TOE.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2 Identification and Authentication

2.2.1 *FIA_ADA.1 Authorized Administrator, Trusted Host and User Authentication Data Initialization*

*FIA_ADA.1.1 The TSF shall provide functions for **initializing authorized administrator, trusted host**, and user authentication data related to [authentication mechanisms identified in F1A_UAU.1 and FIA_UAU.2].*

Inputs:

The vendor's FSPEC , HLD, and/or Administrator Guidance documents should describe the interfaces used for initializing authorized administrator, trusted host and user authentication data and the objects accessed by those interfaces (e.g., a database file) as identified by the authentication mechanisms in FIA_UAU.2

Design Analysis:

The evaluator shall confirm that the vendor's description of the TOE interfaces provided by the TSF, the method of access, and objects accessed by the TSF are complete and consistent with the SFP.

The evaluator must identify the data required by the authentication mechanism and then ensure that an interface to initialize that data exists. The evaluator must confirm that the interfaces pertain to the authentication mechanisms identified in FIA_UAU.2.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, the Administrator Guidance, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that the interfaces provided by the TSF provide functions for initializing authorized administrator, trusted host, and user authentication are consistent with their design. Specifically, the method of access, and objects accessed by the functions must be demonstrated.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FIA_ADA.1.2 The TSF shall restrict use of these functions to the authorized administrator.

Inputs:

The vendor's HLD document should describe the mechanisms that protect the TSF provided used for the initialization of authorized administrator, trusted host, and user authentication data, and that these interfaces are provided only to authorized administrators.

Design Analysis:

The evaluator must ensure that the protection mechanisms described by the vendor are provided by the TSF and can be invoked only by an authorized administrator. The evaluator must identify what constitutes an authorized administrator for this interface, the privileges granted to that role, and how user and trusted host authorization is implemented. Note in requirement FIA.UAU.1 and FIA.UAU.2, the authorized administrator must have an identity that can be authenticated by the TSF and that identity must be authenticated by the TSF before any of the functions identified in this requirement shall be used. Therefore, administrative authorization granted by virtue of being the 'root' user of the system is acceptable as long as the root user is authenticated as an authorized administrator.

The evaluator accomplishes this by examining the Administrator Guidance, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that the functions identified in this requirement are restricted by the TSF from execution by any user other than an authenticated authorized administrator.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.2 *FIA_ADP.1 Basic Authorized Administrator, Trusted Host, and User Authentication Data Protection*

FIA_ADP.1.1 The TSF shall protect from unauthorized observation, modification, and destruction of authentication data that is stored in the TOE.

Inputs:

The vendor's TSP should describe the policy for protecting basic user, administrator and trusted host authentication data from unauthorized observation, modification, and destruction. For example, the TSP should define what is authorized versus unauthorized. Sometimes a policy does not prohibit observation (e.g. /etc/password may be world readable).

The vendor's HLD documentation should describe the mechanisms used for protecting the interfaces that are used for the observation, modification, and destruction of user authentication data.

Design Analysis:

The evaluator must identify the methods used to query, modify, and remove authentication data from the authentication database(s) stored in the TOE. Each method must be provided by a TSF interface and access to the data must be controlled by the TSF.

The evaluator must ensure the access policy enforced on authentication data does not violate the PP requirements.

The evaluator must assess the design to ensure the vendor implemented the policy correctly and completely.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator must verify that the methods used to query, modify, and remove authentication data from the authentication database(s) stored in the TOE are provided only by TSF interfaces.

The evaluator must verify that only the authorized administrator responsible for user authentication data can perform the above operations. The evaluator can achieve this by examining the HLD documentation to identify where the information is stored, in what format the information is contained (e.g., file, database, etc.), what access control mechanism is used to protect the information and how is it enforced. For example, the information may be stored in a flat file within the TOE protected by the underlying operating system's discretionary access control facility (e.g., permission bits). In this scenario the evaluator must demonstrate that access to the flat file is through a TSF interface and the use of the operating system's protection features and are incorporated into the TSF.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.3 *FIA_AFL.1 Basic Authentication Failure Handling*

FIA_AFL.1.1 The TSF shall be able to terminate ***a trusted host, or*** *user session establishment process after* ***[a settable number] of*** *unsuccessful authentication attempts.* ***The failure threshold shall be settable only by an authorized administrator.***

Inputs:

The vendor's FSPEC and HLD documentation should:

- provide a description of the interfaces used to set the attribute that defines the number of allowed unsuccessful attempts by a trusted host to establish a session;
- identify each mechanism that associates failed authentication attempts with a user or trusted host;
- provide a description of the interfaces used to set the attribute that defines the number of allowed unsuccessful attempts by a user or trusted host to establish a session;
- identify each mechanism that associates failed authentication attempts with a trusted host and with a user; and
- provide a description of how each mechanism uses the attribute and the association to prevent session establishment after the threshold has been reached.

The HLD documentation should describe how the trusted host or user session is provided access to the interface for the access control mechanism and how the access is controlled.

The vendor's HLD documentation should define the duration of tracking, the basis of decision (i.e., user ID or host ID), and if the decision is service dependant. For example, if a user fails authentication and exceeds the threshold for a telnet service, does the user still have access to another service such as ftp.

Design Analysis:

The evaluator must identify the interfaces used to set and modify the attributes associated with session termination through TOE HLD documentation. The evaluator must determine what attribute or combination of attributes is used when a decision for session establishment/termination is made and confirm that these attributes can be set and modified through the provided interfaces. The evaluator must identify the mechanism that associate failed authentication attempts with a subject and confirm that the mechanism uses the subject's attribute(s) and the previous association prevents session establishment if the threshold has been exceeded.

The evaluator must identify the security-relevant database that maintains the attribute and confirm that only the administrator can set/modify this attribute. The evaluator can achieve this by examining the HLD documentation to identify where the information is stored, in what format the information is contained (e.g., file, database, etc.), what access control mechanism is used to protect the information and how it is enforced.

The evaluator must identify the mechanism used to terminate the session initiation process and confirm that the mechanism can count the number of session initiation attempts per subject. The evaluator must also confirm that the mechanism is capable of stopping an initiation process when that threshold has been exceeded.

The evaluator accomplishes this by examining the Security Target (ST), the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that a limit on the number of unsuccessful authentication attempts can be established by an authorized administrator. Once the limit is set, tests shall demonstrate that when more unsuccessful login attempts, than the limit allows, are attempted, the session is terminated. Tests shall demonstrate the effectiveness of unsuccessful authentication limits for the attempted authentication of trusted hosts as well as users.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FIA_AFL.1.2 After the termination of ***a trusted host, or*** *user session establishment process the TSF shall be able to disable the* ***corresponding trusted host account or*** *user account until [the session is unblocked by the authorized administrator].*

Inputs:

The vendor's FSPEC and HLD documentation should identify how a user and trusted host are designated as being blocked from further access, where this information is stored, the mechanism used to enforce this, how the block is cleared, and how the ability to clear the block is restricted to an authorized administrator.

Design Analysis:

The evaluator must identify the interface and mechanisms used to set the attribute to enable/disable a user or host account and that the interface and mechanism are part of the TSF.

The evaluator must ensure that only an authorized administrator has access to unblock the user or host account, therefore the evaluator must identify the security-relevant database that maintains the attribute that enables or disable the account and confirm only the administrator can change these attributes.

The evaluator accomplishes this by examining the Security Target (ST), the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, the following:

- the TSF supports the feature of disabling or blocking an account such that once an account is blocked, further service for that account is prevented;
- once the TSF terminates the session establishment process for non-administrator accounts, the TSF shall be able to block the account of the subject attempting to establish the session; and
- the ability of the TSF to disable the subject's account prevents the subject from any subsequent services controlled by the account.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.4 *FIA_ATA.1 Authorized Administrator, Trusted Host, Host and User Attribute Initialization*

FIA_ATA.1.1 The TSF shall provide the ability to ***initialize authorized administrator, trusted host, ,host, and*** *user attributes with provided default values.*

Inputs:

The vendor's FSPEC and HLD documentation should provide a description of the TSF mechanisms used to create an administrator, user, trusted host, or host account and initialize their attributes within the TOE. Vendor documentation should also include a list of attributes associated with a user along with the default values.

Design Analysis:

The evaluator must identify the mechanism used to create a subject's account. Initial attributes associated with an authorized administrator, trusted host, host, or user account may be hard-coded, administratively initialized while the firewall is off-line and no TSP is being enforced, or administratively initialized while the firewall is on-line and the TSF is enforcing the TSP. All are accepted procedures for supplying default values.

The evaluator must be able to determine what the default values are for each attribute. For example, the default values may be initialized during system initialization and each subject will inherit those values on account creation or the default values may be hard-coded in the execution code of the TSF. In either case, the values must be deterministic.

The evaluator must determine which subject attributes have default values. For example, subject identity should not have a default value, however a subject may belong to a default group.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator must confirm the default values are actually set when account creation occurs. The evaluator must also consider that the TSF may contain more than one type of account database.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.5 *FIA_ATD.2 Unique Authorized Administrator, Trusted Host, Host and User Attribute Definition*

FIA_ATD.2.1 The TSF shall provide, ***for each authorized administrator, trusted host, host, and user that is defined to it****, a unique set of security attributes necessary to enforce the TSP.*

Inputs:

The vendor's FSPEC should describe how subjects are uniquely identified within the TSF. The FSPEC should also describe the set of attributes that are assigned to a subject that are necessary and sufficient to enforce the TSP.

Design Analysis:

The evaluator must determine how a subject is uniquely identified. The evaluator must then ensure that the attributes that determine uniqueness are a part of the security attributes.

The evaluator must ensure the set of attributes used to enforce the TSP is unique to a subject.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall, through the execution of tests written by the vendor or the evaluator, create multiple users and determine that each user has a set of security attributes sufficient to enforce the TSP, and unique from all other users, authorized administrator, trusted hosts, and host defined to the TSF.

Tests must be executed that create multiple authorized administrators, users, trusted hosts, **and** hosts and demonstrate that the security attributes for each individual subject is unique from all other subjects.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.6 *FIA_UAU.1 Basic Authorized Administrator Authentication*

FIA_UAU1.1 The TSF shall authenticate any ***authorized administrator's*** *claimed identity prior to performing any functions for the* ***authorized administrator when the authorized administrator accesses the TOE through the console****.*

Inputs:

The vendor’s FSPEC should describe the mechanism used to authenticate an authorized administrator's identity when using the console. The FSPEC should also indicate all functions that support authentication.

Interpretation:

It is acceptable if this requirement is met through a login, an authentication device specific to the console (e.g., biometric device, smartcard), or physical means (e.g., key lock on the console for which the administrator has the key, sign-in sheet witnessed by a supervisor). If console authentication is through a separate authentication device, then that device becomes part of the TSF and the randomness of the authentication information should be reasonably sufficient to prevent the attempts to bypass such devices. As a guide, the device authentication information should be as or more random than an acceptable password system.

Design Analysis:

If the requirement is met through an I&A mechanism through a login sequence, then the TSF login mechanism needs to be understood and documented. The TSF mechanism that performs the authentication and the storage and control of the authentication data needs to be understood and documented. If console authentication is through a separate authentication device then the evaluator needs to understand the functionality of the device and the randomness of the authentication information. If console authentication is through physical method, the evaluator needs to understand and document the method.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, or through physical observation that no individual can perform the functions of authorized administrator even though physical access to the console is available until the individual is authorized as an administrator.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.7 *FIA_UAU.2 Single-use Authentication Mechanisms*

FIA_UAU.2.1 The TSF shall authenticate ***any authorized administrator's, trusted host's, or*** *user's claimed identity prior to performing any functions for the* ***corresponding authorized administrator, trusted host, or*** *user.*

Inputs:

The vendor's FSPEC should describe the mechanism used to authenticate a subject's identity. The FSPEC should also indicate all functions that support authentication.

Design Analysis:

The evaluator must understand the interaction between a service and the authentication mechanism, and how the need for authentication is indicated. For example, a proxy can be configured to require authentication or not. The evaluator must also understand how the TSF associates the need for authentication to specified subjects.

Subjects and services configured to require authentication, are typically subjects from a "remote" host (not co-located within the same physically protected area as the firewall). For those subjects and services, the evaluator must then confirm the authentication mechanism associated with the data identified in FIA_ADA.1 is invoked prior to performing a function.

The evaluator needs to determine if prior to authentication the TSF provides information to the subject and whether publicly disseminated information (e.g., logos, welcome screens, disclaimers, login templates) constitute a function provided to the subject.

The evaluator should determine if unadvertised but valid "wild-card," "factory installed," or "backdoor" authentication material is accepted. Such an attempt should be limited to vendor queries and limited knowledgeable attempts during testing.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, or through physical inspection (for physical access controls at the console) that no subject can perform any function restricted to an authenticated subject until the subject is authenticate. Also, that a subject can perform functions restricted to a specific role (i.e., authorized administrator, trusted host, or user) only after the subject is authenticated in that role.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FIA_UAU.2.2 The TSF shall prevent reuse of authentication data related to [remote authorized administrators, remote trusted hosts, and users requesting the following services:

- *telnet;*
- *ftp;*
- *http;*
- *snmp;*
- *pop;*
- *rlogin;*
- *login].*

Inputs:

The vendor's FSPEC should describe how the authentication data is assigned and protected from reuse (i.e., spoofing or playback of authentication data). If the TSF mechanism(s) that performs these functions differs by service provided then each mechanism and the service for which the mechanism is used should be identified.

Design Analysis:

The evaluator must confirm the data used for the authentication mechanism identified in FIA_ADA.1 cannot be successfully reused. Since, scavenging for authentication data is prevented in requirement FDP_RIP.3, successful reuse of authentication data in this requirement will typically refer to one of three aspects of authentication data.

One, the authentication data is stored by the TSF so that the subject does not have to reauthenticate for each service request once the subject has been authenticated. A reusable password mechanism such as a login/password combination is typically considered unacceptable. This does not mean that the subject must reauthenticate, however if "one-time" authentication is provided, whereby a TSF mechanism performs reauthentication without subject intervention (e.g., single login), the TSF must control authentication information for reauthentication with sufficient integrity.

Two, the integrity of the authentication information must be determined. If authentication information is communicated outside the TSF, either it must be encrypted or it must prevent the ability to determine the original authentication data (e.g., one-time hash, token or similar information).

Three, the probability of one individual using another individual's authentication information is a problem if the authentication material is not sufficiently random (A one-time password function such as that describe by Lamport's Hash or public/private key authentication algorithms will meet this requirement).

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that either authentication material is not reused when requesting one of the services identified in this requirement once initial authentication has occurred, or that if a mechanism within the TSF exists to use reauthentication information generated from authentication information, the evaluator must determine that the original authentication information cannot be determined from the reauthentication information.

The evaluator shall verify, through the execution of tests written by the vendor or the evaluator, that the level of protection claimed for authentication material is indeed being provided and that the mechanism protecting authentication information cannot be bypassed. The evaluator also needs to verify that the mechanism to protect authentication material can only be implemented and disabled by an authorized administrator.

If encryption is used (see requirement FCS_COP.2.1*)*, it cannot be applied at the option of the untrusted user or host (e.g., once authenticated, an untrusted subject cannot change ports to an unencrytpted port unless this is allowed in the TSPl). If a one-time encryption device (e.g., Smartcard, Watchword) is used, procedural controls must be in place so that the requirement to use the device is not at the discretion of an untrusted user or host and procedural controls must be in place for key generation and distribution.

The evaluator must also determine that the randomness of the authentication material is sufficient and it is correctly applied. If passwords are used, the ability to select passwords not easily guessed needs to be determined, especially if no encryption is employed (e.g., locally connected workstations). For instance passwords with a sufficient length should be assigned and tested to see that they work and that an untrusted user cannot alter the password length below which randomness becomes unacceptable.

The evaluator needs to determine if TSF provided information during a failed login attempt compromises the randomness of the authentication material. The evaluator needs to take such TSF provided information into account when evaluating the randomness of the authentication material.

The evaluator needs to determine that vendor installed authentication material does not remain installed when the firewall becomes operational. Often such material is in the form of a vendor installed User-id/password combination that provides all privileges to the individual with the knowledge of this information.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.2.8 *FIA_UID.2 Unique Identification of Authorized Administrators, Trusted Hosts, Hosts, and Users*

FIA_UID.2.1 The TSF shall uniquely identify ***each authorized administrator, trusted host, host, or*** *user before performing any actions requested by the corresponding each* ***authorized administrator, trusted host, host, or*** *user.*

Inputs:

The vendor's FSPEC should provide a description of all attributes that identify a subject and how those attributes provide a unique identification.

Design Analysis:

The evaluator must determine how the TSF associates subject identification with a specific request.

The evaluator must ensure that no mechanisms exist that allow actions pertinent to the enforcement of a SFP to be performed that are not associated with a unique subject identity.

If a group mechanism exists, the evaluator must show how the unique subject identity is mapped to a group before performing any action.

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the FSPEC, and the HLD documentation.

Testing:

The evaluator shall determine, through the review of tests executed by the vendor or the evaluator, if identification material (e.g., User-id) is reused, and if so, how the uniqueness of the user is ensured. The evaluator must determine if multiple subjects can be assigned the same identifier. If unique identifiers are assigned to each subject, the evaluator must determine that the TSF recognizes a significant portion of the entire subject identifier and does not base subject identification on a truncation of the identifier such that uniqueness cannot be guaranteed.

The evaluator must test that unique host identification is guaranteed (e.g., differentiation between hosts on internal networks and external networks).

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.3 Standards-Based Cryptographic Operation

FCS_COP.2.1 The TDF shall perform [encryption of remote administration sessions, compliant with FIPS 140-1 [4]] in accordance with the specific cryptographic algorithm and cryptographic key size which meet the following standard: [FIPS 46-2 and 81: Data Encryption Standard (DES) and DES Modes of Operation [5], [6]].

Inputs:

The vendor's HLD documentation should describe the following information concerning cryptographic modules used in the TSF:

- approval by NIST as a FIPS 140-1[7]cryptographic module;
- specific functional use for each cryptographic module in the TSF;
- interface to the cryptographic module and its invocation sequence;
- security level for all cryptographic modules employed in the TSF.

Design Analysis:

The evaluator needs to understand the installation of the cryptographic module into the TSF so that the evaluator can verify that module interfaces are used appropriately (e.g., TSF responses to operational and state information provided by the module)

The evaluator accomplishes this by examining the Security Target (ST), the TSP, the AG, the FSPEC, and the HLD documentation.

Testing:

The evaluator needs to verify that the all cryptographic modules have been affirmed, in writing, by the manufacturer as complying with FIPS 140-1 and that each cryptologic module has been validated as compliant to the standard by a NIST approved laboratory. Claims that a module is as good as one that is NIST approved against FIPS 140-1, or designed to be approved, are unacceptable. A waiver of FIPS 140-1 granted by a Federal agency to the manufacturer of a cryptologic module shall not apply when satisfying this requirement.

The evaluator needs to determine if the security level of the cryptographic module is consistent with its application for each specific use of a cryptographic module within the TSF. For instance, if a cryptographic module is used to authenticate an authorized administrator, then security level 2 is required.[8]

2.4 Protection of the Trusted Security Functions (TSF)

2.4.1 *FPT_RVM.1 Non-Bypassability of the TSP*

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related operation is allowed to proceed.

[7] FIPS PUB 140-1, "Security Requirements For Cryptographic Modules."

[8] FIPS PUB 140-1, op. cit.,. 19.

Inputs:

The vendor’s FSPEC should include the syntax and semantics for all external interfaces and should identify all interfaces to the TSF, how they are invoked, what objects are accessible through each interface, and how the TSP is enforced across each interface.

Design Analysis:

The evaluator must identify, or confirm the identification of, all of the interfaces provided to the untrusted subjects. For each interface, the evaluator must understand:

- how the interface can be invoked;
- what portion of the TSP is enforced at that interface;
- what are the TSP enforcement mechanisms; and
- what objects are visible across that interface.

The evaluator must analyze the protocols recognized by the firewall to ensure that no message traffic can escape the encapsulation of the protocol. If message data can cause the firewall to perform some action (e.g., take an exception) such that the firewall would execute encapsulated message data, then the TSP could be bypassed.

The evaluator should also attempt to identify undocumented, (not publicly announced, but known to vendor developers and past developers) security relevant interfaces as well as interfaces which do not enforce the TSP. The evaluator’s objective is to ensure that the only way to access an object protected by the firewall is through an advertised interface that correctly enforces the TSP.

Testing:

The evaluator shall verify, through the execution of tests written by the vendor or the evaluator, the existence of undocumented, interfaces to ensure these interfaces cannot interfere with the enforcement of the TSP. If they can then they need to be analyzed as another security-relevant interface provided by the TSF.

The evaluator needs to verify that interfaces which do not appear to participate in the enforcement of the TSP, cannot affect the enforcement of the TSP.

The evaluator must test the protocols to determine that no message traffic can escape the encapsulation of the protocol. Such tests should be limited to protocol flaws in the public domain (noted in vendor publications, published works, and documented on the internet).

The evaluator must verify the services provided by the firewall, if any, prior to authentication do not violate the TSP.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.4.2 *FPT_SEP.1 TSF Domain Separation*

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Inputs:

A domain is the context in which a process operates, including the hardware instructions that it is able to execute and set of objects that it is able to access. The vendor's documentation should include the identification of those hardware mechanisms which could be used to protect objects in the TOE and which of those mechanisms are used to protect the TSF. The vendor's HLD documentation should include an overview of hardware and software mechanisms that implement TSF isolation.

If no untrusted code can execute in the TOE, then the domain of the TSP becomes the TOE. Therefore concerns about domain separation are restricted to concerns about external interfaces. The vendor must identify how the firewall protects itself from external attacks via the network interfaces as well as from such things as specially formulated packets within a message intended to defeat the firewall protection mechanisms.

If untrusted code can execute on the TOE, then the vendor must additionally provide information describing how the TSF maintains a separation of domains between the trusted and untrusted executing subjects (e.g., processes) internal to the firewall platform. An example of untrusted code running on the TOE would include such things as WWW servers and ftp servers running on the firewall.

Design Analysis:

The vendor must identify if untrusted subjects can execute on the TOE. If untrusted subjects cannot execute on the TOE, then the analysis required by the evaluator is more limited and described as follows:

Untrusted code NOT ALLOWED in the TOE

The evaluator must analyze the firewall’s ability to maintain separation of concurrent sessions active on the firewall, between session-oriented and non-session oriented data, and, in general, messages traversing the firewall. The intent is:

- to ensure that the firewall protection mechanisms cannot be subverted or rendered useless from the network interfaces;

- to ensure a packet cannot cause the firewall to perform functions other than those limited to supporting the protocol; and

- to ensure that a message entering the firewall is identical to the message passed to the intended recipient (with the exception of such things as documented packet padding or packet rewriting).

To perform this analysis, the evaluator must review the HLD documentation looking for obvious flaws that an unauthorized subject might exploit to bypass or otherwise defeat the security protection mechanisms of the TSF. Examples of attempts to exploit obvious flaws may include attempts to connect to inactive or undefined ports, attempts to take advantage of documented weaknesses in certain protocols, and attempts to manipulate the size, format or contents of packets in such a way as to bypass the firewall protection mechanisms.

While looking for obvious flaws the evaluator should focus on the following information:

- all interfaces that the TSF makes available to untrusted subjects;

- look for interfaces (documented or undocumented) that do not enforce the TSP, don't enforce the TSP correctly, or allow the bypassing of the TSP; and

- hypothesize ways to formulate packets, request services/connections , or try to exploit know protocol weaknesses to subvert the TSP. (These hypothesis can be verified or refuted during testing.)

The evaluator also performs a thorough analysis of the design documentation, test coverage analysis, and test depth analysis to ensure that testing is performed for TSF isolation with respect to administrative interfaces that manipulate security relevant resources, such as privileged instructions.

Untrusted code ALLOWED in the TOE

If untrusted subjects can execute on the TOE, then the analysis required by the evaluator consists of all analysis outlined above as well as the analysis of the internal architecture of the functions within the TSF (e.g., similar to a TCSEC C2 evaluation).

The evaluator must understand how the TSF maintains a separation of domains between the trusted and untrusted executing subjects internal to the firewall platform. To do this, the evaluator needs to understand the TSF mechanisms that must work correctly to ensure the separation of untrusted subjects from the TSF mechanisms. Some of these mechanisms include the following:

- Separation mechanism between machine states;

- TSF interfaces that run in privileged (e.g., kernel, supervisor) machine state since access to these interfaces provides the ability to violate domain separation;

- TSF interfaces that run in an unprivileged hardware state (e.g., user, problem) but with software privileges (e.g., bypass access controls), since access to these mechanisms often provide the ability to violate domain separation;

- TSF interfaces that run in a semi-privileged state, if one exists, and what authorities/privileges each state conveys to the executing subject, since access to these mechanisms often provide the ability to violate domain separation;

- TSF mechanisms that control domain separation (e.g., process management, memory management, address space control); and

- TSF mechanism that restrict access to interfaces that run in unprivileged machine state, however run with software privileges (e.g., file system management, access controls mechanisms, software privilege application and manipulation).

Testing:

The testing required for this requirement is significantly affected by the presence of untrusted code running in the TOE.

The documents that need to be reviewed to accomplish testing are the: Security Target, the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

Untrusted code NOT ALLOWED in the TOE

When analyzing the design, the evaluator hypothesized ways to formulate packets, request services/connections , that could exploit known protocol weaknesses to subvert the TSP. These hypotheses can now be verified during testing.

As a result of the analysis performed on the test coverage and test depth analysis of the vendor test suite, the evaluator performs whatever additional functional testing is necessary to ensure that all interfaces that manipulate security relevant resources, such as privileged instructions are tested as well as all administrative interfaces.

Untrusted code ALLOWED in the TOE

The evaluator is required to perform the testing described above as well as the following:

Before the testing effort, the evaluator has already analyzed the design as described above and found that, if the TSF is consistent with its design, the belief that separation of domains exists between the trusted and untrusted executing subjects is warranted. The evaluator must determine if the design was faithfully executed.

To do this, all interfaces into the TSF must be tested by either the evaluator or the vendor in a functional test suite that comprises what is typically called **non-security-relevant functional testing** and **security functional testing**.

Non-security-relevant testing of the TSF actually tests TSF interfaces that do not require a policy decision of the TSP. Since these interfaces are part of the TSF, they must work as advertised to ensure domain separation between trusted and untrusted executing subjects; therefore if untrusted code is allowed to execute in the TOE, TSF interfaces that do not require a policy decision are still security-relevant and must be tested.

Security functional testing tests those interface into the TSF that require a policy decision. Security functional testing focuses not only those functions that invoke security mechanisms, but also on the least used aspects of the mechanism using parameters that are at the boundaries of acceptable input. The reason this testing methodology is accepted is these test conditions are often where flaws are found.

2.4.3 *FPT_TSA.2 Separate Security Administrative Role*

FPT_TSA.2.1 The TSF shall distinguish security-relevant administrative functions from other functions.

Inputs:

The vendor's AG documentation should identify all of the security-relevant administrative functions. The TSP and HLD should document how these functions work, what data can be manipulated, how access to those functions is controlled, and how the set of administrative functions are consistent with the TSP and the PP requirements.

Design Analysis:

The evaluator must review the FSPEC, AG documentation, TSP, and HLD documentation to identify:

- all system functions that provide the ability to modify security-relevant data;
- what data can be accessed via those functions;
- how the system identifies those functions as being administrative (i.e., security-relevant) functions;
- how access to those functions is controlled; and
- how the design of these functions and the associated access control mechanisms meet the TSP and the PP requirements.

Testing:

The evaluator shall verify, through the execution of tests written by the vendor or the evaluator, that the TSF will distinguish security-relevant administrative functions from other functions; that access to each function can be controlled as designed; that each such function is restricted access to only the data it is designed to access; and that each security-relevant administrative function performs as expected.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FPT_TSA.2.2 The TSF's set of security-relevant administrative functions shall include all functions necessary to install, configure, and manage the TSF; minimally, this set shall include *[add and delete subjects and objects; view security attributes; assign, alter, and revoke security attributes; review and manage audit data]*.

Inputs:

The vendor's AG documentation should identify the complete set of security-relevant administrative functions available to manage the TSF. The vendor should specifically ensure that a clear description is presented of the administrative functions to add and delete subjects and objects; view security attributes; assign, alter, and revoke security attributes; and review and manage audit data.

Design Analysis:

At this point, the evaluator has reviewed the, FSPEC, AG, and HLD documentation and identified each of the security-relevant administrative functions. Now the evaluator must ensure that this set of functions is sufficient to install, configure, and manage the TSF. The evaluator does this by identifying all of the security-relevant information that needs to be configured and maintained and ensuring that a function(s) exists that provide the ability to manipulate this data.

Testing:

The evaluator shall verify, through the execution of tests written by the vendor or the evaluator, that the TSF will distinguish security-relevant administrative functions that are necessary to install, configure, and manage the TSF. Minimally, this set shall include add and delete subjects and objects; view security attributes; assign, alter, and revoke security attributes; review and manage audit data.

The evaluator will test that administrative interfaces into the TSF and only those administrative interfaces that provide the ability to add subjects and objects, view any or all security attributes of another user, alter any or all security attributes, revoke any or all security attributes, and to manipulate (read, write, modify) the audit data.

The documents that need to be reviewed to accomplish testing are the: FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FPT_TSA.2.3 The TSF shall restrict the ability to perform security-relevant administrative functions to a security administrative role that has a specific set of authorized functions and responsibilities.

Inputs:

The vendor's TSP and HLD should define each of the roles that are supported by their product and what functions can be performed by an individual acting in that role. The HLD should also describe how a user assumes a specific role.

Interpretation:

By requiring two roles, one for authorized administrators and one for a security administrator, Unix superuser cannot be the only admin role. A role must be defined (authorized administrator) that has no su privileges.

Design Analysis:

At a minimum, this requirement requires the definition of administrative and non-administrative roles. The evaluator must:

- identify all roles supported by the firewall and ensure that at least the above two roles are present; and

- identify how the invocation of administrative functions is restricted to the administrative role. For example, it could be based on a group mechanism (all users in the administrators group can invoke the security-relevant administrative functions), a user ID and permissions, user ID and access control lists (ACLs), etc.

Testing:

The evaluator shall verify, through the execution of tests written by the vendor or the evaluator the following:

- a role can be identified and associated with a user or a group of users that have specific, restricted interfaces into the TSF;

- a role can be created that can perform security-relevant administrative functions that cannot be performed by an untrusted subject;

- when an untrusted subject attempts an administrative function, the TSF either returns an access violation or an error attempting an illegal operation;

- for TSF interfaces that can be invoked by administrative and untrusted roles but provide administrative functions when invoked by the administrator, the evaluator must ensure that the for administrative functions provided by the interface are restricted to an administrative role; and

- when a User ID identified with a security administrative role has not been granted access to the correct set of authorized functions and/or the appropriate set of administrative privileges to perform a specific security-relevant function, then any attempt by the role member to perform the function shall fail.

The documents that need to be reviewed to accomplish testing are the: FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FPT_TSA.2.4 The TSF shall be capable of distinguishing the set of ***authorized administrators and trusted hosts*** *authorized for administrative functions from the set of all individuals and systems using the TOE.*

Inputs:

The vendor’s HLD should identify the mechanism used to indicate the role of a subject so that authorized administrators and their specific administrative capabilities are identified in the TSF and their identity and administrative capabilities can be isolated from the description of users.

The vendor’s design should identify the mechanism used to provide unique host identification and how trusted hosts are identified and distinguished from other hosts. Also, the mechanism should be identified that identifies the administrative capabilities associated with each specific trusted host.

Interpretation:

FPT_TSA.2.4 requires that the TSF shall be capable of distinguishing trusted hosts authorized for administrative functions from all systems using the TOE. To meet this requirement it is necessary to identify administrative hosts from systems. The use of the word systems is unclear. *Systems*, used in this requirement are interpreted to mean hosts connected to the firewall.

Design Analysis:

The evaluator must determine what characteristics (attributes) about a subject are used to distinguish that the subject has assumed the role of security administrator. Examples include login name, user ID, group membership, etc.

The evaluator must determine the interface(s) to the TSF that provides administrative capabilities and the capabilities afforded by each such interface.

The evaluator must determine what characteristics (attributes) about a host are used to distinguish the host as a trusted host to perform authorized administrative functions. Examples might be: host name, host ID, network address.

For both authorized administrators and administrative hosts, the evaluator needs to understand the mechanisms that allow administrators and administrative hosts to bypass the TSP.

Testing:

The evaluator shall verify, through the execution of tests written by the vendor or the evaluator, the following:

- login as an administrator, create untrusted users and other administrators, then query the TSF for a list of all users and determine if the TSF can identify the difference between untrusted users and administrators;

- login as an administrator, create hosts and trusted hosts in the administrative database (can be a logical entity), then query the TSF for a lists of all internal hosts and determine if the TSF can identify difference between hosts and trusted hosts;

- login as the only authorized administrator (previously established at install) and attempt to remove administrative privileges from your own User-id stored in the administrative database. It would be best if this is not allowed, but if it is allowed log-off and login once again as the same administrator. Now test if the evaluator still has administrative capabilities. If so, determine how this was possible and if this requirement was met. If not determine that the TOE can only be administered by reinstalling the TSF.

- login as an administrator and attempt to add an untrusted user with the same User-id. If this is allowed, determine how the TSF differentiates between the untrusted user and the administrator. Also determine how requirement FIA_UID.2, *Unique Identification of Users*, was satisfied;

- create a record in the administrative database that identifies a trusted host, then communicate to the firewall with all of the attributes of a trusted host. Examples might be: host name, host ID, network address. Confirm that the TSF believes the connection is from a trusted host. Then attempt to connect from an external untrusted host with the same attributes. Determine if this is possible. If it is not, no further activity for this test is necessary. If it is possible, determine how the TSF is capable of distinguishing between the trusted host and the external untrusted host.

- once an administrator is authenticated the administrator is restricted from executing untrusted code, therefore the evaluator should attempt to execute an untrusted program after being authenticated as an administrator;

- login as an untrusted user and attempt to execute an administrative interface, the attempt should either provide an access violation or abort as an attempted illegal operation.

  The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FPT_TSA.2.5 The TSF shall allow only ***authorized users and trusted hos****ts to assume the security administrative role.*

Inputs:

The vendor’s HLD should indicate how the attributes which identify that a subject has assumed the security administrative role, are assigned to an interactive session and how they are protected.

Design Analysis:

For authorized administrators, the evaluator must perform the following:

- identify and understand the role assumption mechanism;

- understand how the role assumption checks subject authorization before allowing the assumption of the administrative role;

- understand how the role assumption mechanism sets the attributes indicating the user has assumed the administrative role; and

- ensure that there is no way to forge the attributes that indicate that a user has assumed the security administrative role.

For authorized administrative hosts, the evaluator must perform the following:

- identify and understand the mechanism by which an administrative host is identified

- determine how the TSF reliably authenticates a host identifier used to identify a host with administrative capabilities, so that some other network source is not masquerading as an administrative host; and

- understand the role of an administrative host.

Testing:

The evaluator shall, through the execution of tests written by the vendor or the evaluator, perform the following:

- establish an authorized user with only the access and privileges required for that role;

- demonstrate that a specific user is identified as an authorized user and the distinction between an untrusted user and the authorized user;

- demonstrate that a user that is an authorized user can assume the security administrative role; and

- demonstrate that a user with every possible access and privilege that are not equal to, or a superset, of the accesses and privileges associated with an authorized user cannot assume the role of the security administrator.

- demonstrate how a trusted host is uniquely identified;

- establish a trusted host with the necessary identification;

- demonstrate a trusted host may assume the security administrative role; and

- demonstrate a host with all identification attributes of a trusted host except one cannot assume the role of the security administrator (e.g. if a trusted host is identified by host-ID, ip address, and port number, then a host with the correct ip address and port number but an incorrect host-ID would be prevented from assuming the role).

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FPT_TSA.2.6 The TSF shall require an explicit request to be made in order for ***an authorized administrator or trusted hos****t to assume the security administrative role.*

Inputs:

The vendor's HLD and Administrative Guide should identify how a user requests the assumption of the security administrative role. The vendor's HLD should identify the specific required communication sequence a host communicates to the firewall to become an authorized administrative host.

Interpretation:

Throughout FPT_TSA.2 (*FPT_TSA.2.1- FPT_TSA.2.6*) the term security administrator is used. It is assumed that only the security administrator can perform security-relevant administrative functions. It is also assumed that no untrusted users exist on the firewall[9]. Therefore, it must be concluded that there are administrators who are not security administrators and who can assume the role of the security administrator. Please note that in requirement FPR_TSA.2.4, the set of all individuals is interpreted to mean the set of all authorized administrators, since no one else can access the traffic filter firewall. In FPR_TSA.2.6, it is clear that an authorized administrator is not the same as the security administrator.

It is anticipated that application level firewalls may only provide a single administrator role that can perform all administrator functions. According to the requirements levied in FPT_TSA.2, such a firewall is unacceptable.

Design Analysis:

The evaluator must understand the TSF mechanisms that provide an interface to service an explicit request to assume administrative capabilities, both for a user and a host, to determine if an explicit request is required.

The evaluator must identify all of the ways that a user can assume the security administrative role and ensures that each way requires an explicit action. For instance, any combination of the following could provide an administrative interface:

- login with the identity of an administrator;
- login as an untrusted user and invoke a protected interface (e.g., assume the role) that provides administrator capability;
- invocation of a protected program that provides administrative capabilities; or

[9] See Section 1.3, Firewall Security Policy.

- invocation of a command or system call (e.g., Add User) that implicitly adds that user to an administrative group.

The evaluator must understand the specific required communication sequence a host communicates to the firewall to become an authorized administrative host.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, every method available for a user to become an authorized administrator. It must be demonstrated that an authorized user must perform an explicit action to become assume the security administrator role, and it also must be demonstrated that a person other than an authorized administrator performing any action , including the explicit action identified above, must be precluded from becoming an authorized administrator (e.g., if the console is in a controlled area with access restricted to an authorized administrator and other personnel, and access to the console provided administrator privilege, the TOE would not meet this requirement)

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.4.4 *FPT_TSM.1 Management Functions*

FPT_TSM.1.1 The TSF shall provide the authorized administrator with the ability to set and update [security relevant administrative data], ***and to enable and disable user authentication for the services in FIA_UAU.2.2.***

Inputs:

The vendor’s HLD should identify and describe the functions used to manage the security relevant administrative data and to enable and disable user authentication for services identified in FIA_UAU.2.2.

The HLD should explicitly identify and describe the functions that provide the capability to specify subjects requiring authentication prior to being granted access to any services.

The vendor’s Administrative Guide should identify and describe the administrator interface to set and update security relevant administrative data, and to enable and disable user authentication for services identified in FIA_UAU.2.2.

Design Analysis:

The intent of the above statement is to require that an authorized firewall administrator is provided the ability to configure the firewall to implement an organization’s specific firewall security policy. The previous family of requirements already discussed the required evaluator actions necessary to ensure a controlled ability to administer the firewall. The only new requirement added by the above statement is to provide an ability to enable and disable user authentication for the services in FIA_UAU.2.2. To ensure the satisfaction of this requirement, the evaluator must:

- identify the attribute(s) that indicate that a user is to be authenticated prior to receiving access to firewall protected services (authentication service attributes);
- identify how those attributes are enabled, updated, and disabled;
- identify how the settings of those attributes are protected and can only be manipulated by an authorized security administrator; and
- identify how the firewall uses those attributes to ensure that designated subjects are authenticated.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, the following:

- test that authentication service attributes are restricted to an authorized administrator, and that the administrator can enable them and disable them;
- test that a user is not provided authentication services before authentication service attributes are enabled by an administrator, then test that a user is provided authentication services after authentication service attributes are enabled, then test that the user is not provided authentication services once the administrator disables authentication service attributes;
- test that the authentication service attributes actually provide authentication services to the granularity of a single user; and
- test that no other attributes of a user that are controlled by the TSF, other than the authentication service attributes identified in analysis provide authentication services to a user.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FPT_TSM.1.2 The TSF shall provide the authorized administrator with the ability to perform [installation and initial configuration of the firewall; functions that allow system start-up and shutdown; backup and recovery]. ***The backup capability shall be supported by automated tools.***

If the TSF supports remote administration from either the internal or external interface, the TSF shall:

a) Have the option of disabling remote administration on either or both interfaces.

b) ***Be capable of restricting the address from which remote administrator actions can be performed.***

c) ***Be capable of protecting the remote administration dialogue through encryption***

Inputs:

The vendor’s HLD and Administrative Guide should describe the functions available to install, configure, startup, shutdown, backup, and recover the system.

The documentation should describe the administrative interface(s). If the ability to remotely administer the firewall exists, the vendor should describe how to restrict their use based on source address or disable them altogether.

The documentation should also describe the TSF mechanisms that implement encryption for remote administrative dialogues, and the sequence of events required by an administrator to establish a remote administration dialogue through encryption.

Interpretations:

The DTR authors have assumed that the above statement should not have applied the term “authorized administrators” to the installation and initial configuration portion of the above requirement since there is no way for the TSF to identify an authorized administrator before it is installed and an administrator account defined. It is likewise not possible for the TSF to protect itself from all methods of shutdown by a non-administrative user (e.g., powering down the system). The ability to start-up, backup and recover the system, and establish remote administration should be restricted to authorized administrators.

For automated backup tools, the DTR authors have adopted a loose interpretation of automated tools and assumed that the use of scripts, batch jobs, operating system provided backup tools, etc. will meet the intent of this requirement.

Design Analysis:

The evaluator must review the HLD and Administrative Guide to ensure that tools have been provided that allow the firewall to be installed, configured, started, shutdown, backed up and recovered. The evaluators must also identify all interfaces to the administrative functions and, if remote interfaces exist, verify that their use can be controlled in accordance with this requirement. The evaluator identifies the attributes that are used to specify the allowed access to the remote administrative interfaces and the mechanism(s) that make use of those attributes to control access to these interfaces.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, the following:

- The evaluator, acting as an administrator must be able to install and perform the initial configuration of the TOE using the instructions found in the AG document(s). If instructions are incomplete, then this test fails. The installed TSF should be the representative TOE used in all testing.

- Once installed, the evaluator needs to perform start-up, and shut-down procedures to ensure they comply with expected results. After shutdown the TOE must be left in a state that start-up can be successfully retested.

- Once the TSF is installed, the backup and recovery capability must be tested on the installed TSF.

- All features of the automated tools documented in the Administrative Guide need to be tested. This does not mean that every feature needs to be exhaustively tested as long as the evaluator is convinced that the feature works correctly.

- If the TSF supports remote administration from either an internal or external interface test on each supported interface, and on all supported interfaces (external and internal) functioning at the same time. Perform testing on specific workstation(s), identified by address, connected to each type of interface. The following must be tested:

  - attempt remote administration from each interface before it is enabled from connected workstation(s);

  - enable remote administration at each interface such that the administrator is able to perform this function from the same workstation(s);

  - perform a sample of administrative functions from the workstation(s) to ensure remote administration is indeed functioning;

  - enable encryption such that the dialogue between the workstation(s) and the TSF is encrypted;

  - perform a sample of administrative functions while encryption is in operation;

  - disable remote administration;

  - attempt to perform administrative functions from the same workstation; and

  - attempt to perform remote administration from another workstation to ensure that the entire service has been disabled and not just for a specific workstation.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.5 FAU Security Audit

2.5.1 *FAU_GEN.1 Audit Data Generation*

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) *Start-up and shutdown of the audit functions.*

b) *All auditable events relevant for the basic level of audit defined in all functional components included in the PP/ST**, which are identified as "basic" or "minimal in Table 2.2.***

c) *Based on all functional components included in the PP/ST, the events indicated as "extended" in Table 2.2 .*

Inputs:

The vendor's HLD and Administrative Guide should identify all of the firewall system's auditable events and map them to the events listed in this requirement and in Table 2.2.

Design Analysis:

The evaluator must review the HLD and Administrative Guide to ensure that the TSF is capable of auditing the types of events identified in FAU_GEN.1 and Table 2.2.

The evaluator must examine the audit trail to confirm that the events the vendor has stated the TSF is capable of auditing are recorded.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that each specified auditable event generates an audit record when the event is being audited and when the event actually occurred. To perform this verification, tests must exist that generate audit records for each auditable event identified in this requirement. The evaluator needs to review the audit log and compare the audited event(s) with the known information about the actual event to ensure auditing is being performed correctly.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) *Date and time of the event, type of event, subject identity, and success or failure of the event.*

b) ***Additional Information specified in column four of Table 2.2** for each audit event type based on the auditable event definitions of the other functional components included in the Protection Profile and/or Security Target.*

Inputs:

The Administrative Guide should identify what information can be captured in the audit trail. In the Security Target, the HLD, the vendor should identify the TSF interface(s) that cause an audit record to be written.

Parent Family	Level	Auditable event	Additional Audit Record Contents
FAU_MGT	basic	Any attempt to perform an operation on the audit trail, including shutdown of the audit functions/subsystem.	Object ID of the audit trail object affected, if applicable
FAU_PRO	basic	Any attempt to read, modify or destroy the audit trail.	
FDP_ACF	basic	All requests to perform an operation on an object covered by the SFP.	The object ID of the affected object.
FDP_SAM	basic	All attempts to modify security attributes, including the identity of the target of the modification attempt.	
FDP_SAQ	basic	All attempts to query security attributes, including the identity of the target of the query.	
FIA_ADA	basic	All requests to use TSF authentication data management mechanisms.	
FIA_ADP	basic	All requests to access authentication data.	The target of the access requested.
FIA_AFL	extended	The termination of a session caused by a number of unsuccessful authentication attempts that exceed the threshold setting.	
FIA_ATA	basic	All requests to use the attribute administrative functions.	Identification of the user attributes that have been modified
FIA_UAU	basic	Any use of the authentication mechanism.	
FIA_UID	basic	All attempts to use the identification mechanism, including identity provided.	
FPT_TSA	minimal	Use of security-relevant administrator function.	

FPT_TSM	basic	Successful and unsuccessful attempts to modify (set and update) TSF configuration parameters.	The new values of the configuration parameters.

Table 2.2. Auditable Events

Interpretation:

There appears no requirement that the TOE must allow all auditable events to be audited at the same time. This situation actually exists on a commercial C2 product where the number of auditable events is larger than the audit mask, so that all auditable events can be audited, but only a subset at any given time.

Design Analysis:

The evaluator must review the Administrative Guide to determine if all of the information required by FAU_GEN.1.2 is recorded in the audit trail. The evaluator should also review the text of Table 2.2 to identify other information that must be captured in the audit trail.

The evaluator must examine the audit trail to confirm the required information has been recorded.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that each auditable event can be audited, and the evaluator must verify through inspection of the audit log that all of the required information was recorded.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.5.2 *FAU_MGT.1 Audit Trail Management*

FAU_MGT.1.1 The TSF shall provide the authorized administrator with the ability to create, archive, delete, and empty the audit trail.

Inputs:

The vendor’s HLD documentation should identify all TSF interfaces that provide the capability to create, archive, delete, and empty the audit trail. The vendor should describe how each of these interfaces are protected and restricted for use by the authorized administrator.

The vendor should identify all the forms in which audit data is stored and all TSF locations in which audit data is stored. That is, the vendor lists the auditable events; for each event, the vendor describes the format of the audit trail record and identifies the file(s) in which the record is stored. For a TSF with multiple audit files, the vendor's describes whether and how all audit data is eventually consolidated in a single unified audit trail.

The AG document(s) should describe the services advertised to initialize and control the audit subsystem, describes any procedures for selective use of the audit mechanism (e.g., how to set audit parameters to capture or to exclude from capture specific events), and describes how to archive, retrieve, and analyze the audit trail.

Interpretation:

In requirement FPT_TSA.2, a security administrator is a specific role that can be assumed by an administrator. A security administrator is a different subject than an administrator. In requirement FPT_TSA.2.2, only the security administrator can review and manage audit data. However in this requirement, there is no mention of a security administrator; therefore it is interpreted that any authorized administrator can perform the functions in this requirement and somehow creating, archiving, deleting, and emptying the audit trail is not the same activity as managing the audit data.

Design Analysis:

The evaluator must review the HLD and Administrative Guide to confirm that the required audit trail management functions exist. The evaluator must also identify how access to use the audit trail management functions is controlled and restricted to the administrative role.

In the event that the audit data is maintained on a separate system (for example, some routers do not have sufficient internal storage to record audit events and provide the ability to write audit data to a separate system) the evaluator must consider that system to be included in the TSF and ensure that it provides sufficient mechanisms to manage and protect the audit trail.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, the following:

- test that the identified management functions are restricted to the administrative role;

- following the administrative guide, test that each management function exist, and that at least one administrative interface performs the following:

    - creates the audit trail such that the TSF function(s) that perform audit can and will write audit records to the audit trail created by the administrator;

    - archives the audit trail to a backup device such that the archived audit trail can be viewed and understood by the administrator using whatever tools are identified for this purpose in the administrative guide;

    - deletes the audit trail; and

– empties the audit trail such that the abstraction that contains the audit trail (e.g., file, data set, cache) still exists, but subsequent to the performing this function, no logical entries remain in the audit trail.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.5.3 *FAU_POP.1 Human Understandable Format*

FAU_POP.1.1 The TSF shall provide the capability to generate human understandable presentation of any audit data stored in the permanent audit trail.

Inputs:

The vendor's Administrative Guide should describe how to view the audit trail data in a human readable format (hexidecimal is unacceptable). The vendor should provide an argument why it is believed that a presentation of the audit data can be generated that an administrator employing a **reasonabl**e level of effort can reconstruct audited events.

Design Analysis:

The evaluator must review the Administrative Guide to identify how to view the audit data and determine if the capability exists to present stored audit data in a form whereby an administrator employing a **reasonable** level of effort can reconstruct audited events.

Testing:

The evaluator must examine the audit trail to confirm that the information is presented in a human understandable format. A test of reasonableness needs to be applied here. It is unreasonable to expect the administrator to read hexidecimal and recreate activity of one user during one session, even though the administrator may be able to read hexidecimal. It is unreasonable to expect the administrator to read an audit log in continuous ascii text for all records associated for one day, without some record grouping, in an attempt to recreate the activity on one port for one day. The minimum retrieval capability of the audit review tool is described in requirement FAU_SAR.3.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.5.4 *FAU_PRO.1 Restricted Audit Trail Access*

FAU_PRO.1.1 The TSF shall restrict access to the audit trail to the authorized administrator.

Inputs:

The vendor describes which TSF processes are authorized to access the audit data and how the audit data is protected from unauthorized access.

The vendor needs to identify where the audit log is stored. If all audit records are stored on the firewall, the vendor needs to identify this. If part, or all, of the audit log is stored on a server elsewhere in the network, the interface used and the host on which the audit log is stored should be identified. Since the audit log is part of the TSF and must be protected from untrusted subjects, the vendor should describe how the audit log is protected.

If the audit log is stored and/or retrieved through a DBMS, then the DBMS needs to considered another TSF and the vendor should provide sufficient information to demonstrate that the audit log can be protected by the DBMS.

Interpretation:

Since the word “access” is used in the requirement, it is assumed that only authorized administrators are provided read access to the audit file even though read access is provided to untrusted subjects in another DTR with higher assurance, and even though no read access is provided administrators in requirement FAU_MGT.1.1 where administrative access is only defined for create, archive, delete, and empty the audit trail, but no administrative interface is required to read the audit file. Also, it is assumed that the TSF routines that write to the audit trail are allowed to have access to it.

Design Analysis:

The evaluator must confirm that the audit trail is adequately protected by the TSF from unauthorized access to the audit data. If the audit log is stored on a host (e.g., one or more file servers) other than the firewall (audit log host), then the communication between the firewall and that audit log is sufficiently protected to restrict access to the administrator. One method to protect the communication with the audit log host is through encryption. The audit log host must provide the same, or higher, assurance that the audit log is protected.

The evaluator must confirm that the TSP identifies conditions under which access to the audit trail is authorized. Typically, access to the audit trail is restricted to privileged users or applications. The evaluator confirms that the mechanisms that restrict access to the audit trail (e.g., DAC protection with access given only to authorized users) are consistent with the policy.

If the audit log is stored on an audit log host, access by the administrator, logged into the firewall, must be somehow authenticated on the audit log host even though encrypted communication is used to write to the audit log and by the administrator when querying the audit log. If the audit log host requires the administrator to login to it (thus performing local I&A), some firewall and/or audit log host TSF mechanism must exists that assures only a firewall administrator can log into the audit log host as the firewall administrator to gain access to the firewall’s audit log.

If the audit log is stored and/or retrieved through a DBMS, then the DBMS needs to considered another TSF and the evaluator must perform as detailed a design analysis on the DBMS as would be performed on other TSFs. The evaluator must understand how the audit log is protected by the DBMS.

To perform design analysis, it is necessary for the evaluator to examine the Security Target (ST), the TSP, the FSPEC, and the HLD documentation of the firewall.

If a DBMS is used to store/retrieve information in the audit log, appropriate information about the DBMS needs to part of the ST, the FSPEC and the HLD documentation.

If an audit log host is employed to store audit information, similar information for this host must be examined.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that no access is provided to any subject other than the administrator and the TSF routines that provide an interface into the audit trail.

The evaluator should attempt to manipulate each interface into the audit trail as a user with privileges/capabilities other than the authorized administrator.

If the audit log is stored on audit log host(s), the evaluator must determine that encryption meets all requirements of FCS_COP.2.1, and that the firewall administrator can be identified and authenticated by the audit log host as the firewall administrator with access rights to the firewall audit log.

If the audit log is stored and/or retrieved through a DBMS, then the DBMS needs to considered another TSF and the evaluator must perform as detailed a design analysis on the DBMS as would be performed on other TSFs.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results of the firewall and similar information for the audit log host, if the audit log is stored remotely.

2.5.5 *FAU_SAR.1 Restricted Audit Review*

FAU_SAR.1.1 The TSF shall provide audit review tools, with the ability to view the audit data.

Inputs:

The vendor's Administrative Guide should describe the mechanisms used to view the audit data.

Design Analysis:

The evaluator must confirm the mechanisms to view the audit data are described adequately such that if used as described they will meet this requirement. Regardless where the audit log is stored (firewall or audit log host, the evaluator must determine that if an event occurs on the firewall and it is to be audited (see FAU_SAR.3.1), that event can be reconstructed accurately, (e.g., with appropriate information and in an intelligible time sequence). It is unacceptable for the firewall administrator to use audit review tools that provide multiple independent streams of information (e.g., one for each location where a part of the audit log is stored), which require manual integration and sequencing before an audited event can be reconstructed.

Testing:

The evaluator shall confirm, through the review of tests executed by the vendor or the evaluator, that the mechanisms **as described** by the vendor for viewing audit data allow such an action to occur. Mechanisms should only be used as specified in the description provided by the vendor. If multiple audit logs must be reviewed to reconstruct an audited event, the evaluator must test that the audit viewing tool performs the coordination and sequencing of the audit records so that the administrator is provided a single response to a request to view a single audited event.

FAU_SAR.1.2 The TSF shall restrict the use of the audit review tools to the authorized administrator.

Inputs:

The vendor describes which accounts or roles are authorized to use the audit review tools and how the review tools are protected from unauthorized use.

Design Analysis:

The evaluator must confirm that the use of the audit review tools is adequately protected by the TSF.

The evaluator must confirm that the TSP identifies conditions under which access to execute the audit review tools are authorized.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that audit review tools can be used by the authorized administrator and that audit review tools cannot be used by any subject other than the authorized administrator.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.5.6 *FAU_SAR.3 Selectable Audit Review*

FAU_SAR.3.1 The TSF shall provide audit review tools with the ability to perform searches and sorting of audit data based on:

- [Subject ID;
- Object ID;
- Date;
- Time;
- Some combination of the previous bulleted items].

Inputs:

The vendor's Administrative Guide should provide a description of the audit review tools capabilities in terms of performing searching and sort of audit trail data.

Design Analysis:

The evaluator must understand the capabilities of audit review tools and determine if the capabilities specified in this requirement appear to exist

Testing:

The evaluator must confirm the audit review tools provided in the TSF allow the administrator to search the audit data on the security attributes listed above.

The evaluator must confirm the audit review tools provided in the TSF allow the administrator to sort the audit data on any security attributes listed above.

The evaluator must confirm that searching and sorting can be performed with combinations of the above security attributes that specifically includes access by individual subjects to specific objects.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

2.5.7 *FAU_STG.3 Prevention of Audit Data Loss*

FAU_STG.3.1 The TSF shall store generated records of audit in a permanent audit trail.

Inputs:

The vendor should identify in the Administrative Guide where the audit trail data is stored. If there are more than one audit trail, the location of each audit trail and the identity of the types of records stored in each audit trail should be identified.

Design Analysis:

The evaluator needs to confirm that the identity of the audit trail location is revealed and if multiple locations exist, that each is revealed, and the evaluator must assess if permanent storage is used for each location. If the audit data must be stored on a secondary system to satisfy this requirement, the system on which the audit data is stored must be considered as part of the TSF.

The evaluator must determine that all locations are documented in the Administrative Guide.

Testing:

The evaluator must confirm that there is the ability to store the audit data in non-volatile storage.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FAU_STG.3.2 The TSF shall limit the number of audit events lost due to failure and attack.

Inputs:

The vendor is expected to include in the AG documentation an analysis of the amount of audit data and a description of the audit data that can be lost in the event of a system failure. The description might include a statement identifying that the last events audited up to the limited can be lost. Or if multiple audit files/logs exist, the vendor should categorize the type of data lost for each audit file/log. If the audit trail is distributed over multiple networked connected nodes, then the impact of losing a connection should be described.

Design Analysis:

The requirement requires the vendor to take some action to prevent the loss of audit data. The evaluator needs to determine that the vendor has performed the analysis and the evaluator will report the expected loss if the vendor does not provide this information in the AG documentation. The evaluator must ensure that the loss of audit data is not unlimited.

The evaluator must confirm that the AG documentation identifies circumstances where there is a potential for audit data loss. Each circumstance should be accompanied by an approximate quantity of audit data that may be lost.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that the vendor's analysis of the amount of audit data that could be lost is reasonably accurate and indeed it is not unlimited. [10]

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

FAU_STG.3.3 In the event of audit storage exhaustion, the TSF shall be capable of preventing the occurrence of auditable[11] actions, except those taken by the authorized administrator.

[10] Typically the amount of audit data that can be lost is validated by creating a very small audit log, then writing known records to the audit log, and cause an event to occur that will cause the loss of audit data (e.g. overwrite the audit log, turn power off). Next the known records are compared to the record in the audit log. As long as all records were not lost, the amount of audit data lost was limited.

Inputs:

The vendor is expected to describe the steps taken by the TSF when the storage limit of an audit log is reached. This includes the steps taken by the TSF responsible for saving the audit log and assigning a new resource for continued audit activity (e.g., audit data management) as well as this information that describes how the TSF senses resource exhaustion of the audit storage and prevents further audited events.

Interpretation:

The satisfaction of this requirement will depend upon the action taken by the TSF once an audit trail is full. When an audit trail is overwritten one of three events typically happen:

1. the TSF audit functions realize the audit trail is full, interrupts the currently running process, saves the state of all queued processes, interrupts the currently running process, assigns a new audit log before another audited event is written, and then resumes processing; all without external intervention;

2. the TSF realizes the audit trail is full, sets a high priority interrupt and waits for external intervention;

3. the audit trail becomes full and the system crashes.

In each case, the TSF may be able to prevent the occurrence of further auditable actions until another valid audit log is ready; however the intervention of the authorized administrator may not be necessary.

In the first case, no intervention can occur (the system corrects the problem without the loss of audit data), therefore this case appears unacceptable since no intervention of the authorized administrator took place.

In the second case, the TSF is waiting for external intervention and as long as intervention is provided by the authorized administrator, this case is acceptable.

In the third case, the system crashed. As long as the authorized administrator is the only person that can restart the system and create a new audit trail before any additional audited events are generated, then this condition is acceptable.

Design Analysis:

The evaluator needs to understand the actions taken by the TSF when the storage capacity of an audit log is exhausted. The evaluator must confirm that the firewall system will not perform any auditable actions, other than those taken by the authorized administrator, once the audit storage is exhausted. Even though transient audit information may be lost

[11] Actually an auditable event can never occur, since auditable events are those with the ability to be audited. The requirement is referring to any auditable event for which the TSF has been instructed to audit, thus the event has become an audited event.

(FAU_STG.3.2), the evaluator needs to validate that no further auditable events occur until additional audit storage resources are available**.**

The evaluator identifies how the firewall system prevents auditable actions once the audit storage is exhausted. For example, the first action an auditable function tries to perform is a write to the audit trail, which will fail and cause that process to wait or exit upon that failure.

Testing:

The evaluator shall verify, through the review of tests executed by the vendor or the evaluator, that in the event of audit storage exhaustion, the TSF shall be capable of preventing the occurrence of auditable actions, except those taken by the authorized administrator.

Typically the satisfaction of this requirement is validated by creating a very small audit log, then writing records to the audit log until a write to the audit log causes and overwrite of the audit log. Once this happens the evaluator needs to verify that the first auditable event (Table 2.2. Auditable Events) that can occur must have originated from a subject acting on behalf of the authorized administrator.

The documents that need to be reviewed to accomplish testing are: the FSPEC, Test Coverage Analysis, test plans, test procedures, and test results.

3. Assurance Requirements

Assurance is defined as the, " property of a TOE giving grounds that its security functions enforce the TSP." In other words, assurance does not describe the requirements for the mechanisms that provide the security features, (they are described in this DTR). Rather, assurance requirements are placed on the TOE so the customer can determine how much trust should be placed in **the mechanisms functioning as advertised.**

The Common Criteria provides for four levels of assurance. Although each level of assurance is not exactly a superset of the preceding level, each level does provide a higher level of trust. The levels of assurance are EAL1 through EAL4. EAL1 (Functionally Tested) is the lowest level of assurance. EAL1 provides the consumer with the assurance that the product actually exists and is operational. EAL2 is the next higher level of assurance and is the level of assurance required by the Traffic Filter Firewall DTR.

EAL2 (Structurally Tested) is the highest assurance level that imposes only minimal additional tasks on the developer (additional to the tasks typically performed during development by some vendors). HLD documentation is required, whereas detailed design documentation is not required. The HLD documentation describes the security functionality provided by each subsystem of the TSF (subsystem is a logical or physical decomposition of the TSF) and the interfaces into a subsystem. EAL2 only requires testing at the FSPEC, therefore interfaces are only tested to see if they work as advertised; no attempt is made to try to circumvent or manipulate an interface in ways not advertised in the vendor's literature.

The EAL2 assurance requirements levied on the developer for the Traffic Filter Firewall are summarized in the following table[12].

[12] This table will need to be updated when the Assurance DTR is finalized. Currently this table is in that document, however all guidance documents are not identified in the table.

Assurance Class	Assurance Components
Configuration Management	ACM_CAP.1 Minimal Support
Delivery and Operation	ADO_IGS.1 Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1 TOE and Security Policy ADV_HLD.1 Descriptive High-level Design ADV_RCR.1 Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1 Administrator Guidance
Tests	AGD_USR.1 User Guidance ATE_IND.1 Independent Testing - Conformance ATE_COV.1 Complete Coverage - Informal ATE_DPT.1 Complete Coverage- Informal ATE_FUN.1 Functional Testing ATE_IND.1 Independent Testing-Conformance
Vulnerability Analysis	AVA_SOF.1 Strength of TOE Security Function Evaluation AVA_VLA.1 Developer Vulnerability Analysis

Table 3 Assurance Requirements - EAL 2

The discussion of the evaluator guidance and recommended action to determine the compliance of a product to the assurance requirements for this PP are specified in the Assurance DTR [13].

[13] Common Criteria Testing Program Derived Test Requirements For EAL1 Through EAL3, draft 11, March 1998.

4. Related Documents

Common Criteria for Information Technology Security Evaluation, Common Criteria Editorial Board. Version 1.0, 31 January 1996.

Common Criteria Testing Program Derived Test Requirements For EAL1 Through EAL3, draft 29, September 1997.

Derived Verification Requirements for TCSEC C2: Controlled Access Protection, National Security Agency, Trust Technology Assessment Program (TTAP), Pilot Version 1.0, January 1997.

Milkyway Networks Black Hole Firewall, Version 3.01E2 for SPARCstations, Final Evaluation Report, Communications Security Establishment, Canada, November 1997.

Network/Transport Packet Filter Firewall (PFFW) PP, Common Criteria, Version 1.0 Part 4, Predefined Protection Profiles

Process Action Team (PAT) Guidance Working Group, Form and Content of Vendor Test Documentation, National Computer Security Center, Fort George G. Meade, Maryland, 2 July 1993. *For Cryptographic Modules*, National Institute of Standards and Technology, FIPS-PUB 140-1.

Security Requirements January 11, 1994

Test Requirements For Commercial Database Management Systems (CDBMS) Protection Profile (Draft), National Institute of Standards and Technology, December 8, 1997.

US Government Application Level Firewall Protection Profile for Low Risk Environments, Version 1.0, December 1997.

5. Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
FSPEC	Functional Specification
HLD	High-level Design
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy